REMARKS

Claims 1-12 are pending in this application, with claims 1, 7 and 11 being independent. Favorable reconsideration of the action is respectfully requested in view of the following comments of the Applicant, which are preceded by related comments of the Examiner in small bold type:

Claim Rejections – 35 USC § 102

Claims 1-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Challener et al. (U.S. Patent 6,718,468).

Amended claim 1 is directed to a computer-implemented method for a secure transaction that includes generating a first key from a user-supplied unencrypted password provided by a user computing device. The method also includes encrypting the user-supplied unencrypted password using the first key, and creating a user record. The method also includes storing the encrypted password in the user record.

In the current action, the Examiner states that the "cited prior art does implement and teach a system that relates to generating of password-encrypted key form a user-supplied password...." Applicant disagrees.

Challener simply uses a public/private key, which is not described as being produced from user supplied information, to encrypt a password (and the encrypted password is stored). At a later time, the encrypted password is retrieved, de-encrypted and compared to another password from a user (presumably provided to gain access to a system, for example). However, nowhere does Challener disclose or suggest "generating a first key from a user-supplied unencrypted password provided by a user computing device" and "encrypting the user-supplied unencrypted password using the key", as required by independent claim 1.

Rather to start his process, Challener states that each user has a public/private key. In this regard, a cited portion of the reference reads:

> Each user of computer system 10 has a separate and unique user public/private key pair established for each application within computer system 10. The term "user" is understood to mean a person, a service, an application, a device, or any other entity that may access an application. The term "user" is not limited to a human user. A certificate may be established within computer system 10 for a user to access a particular application. The certificate may be specifically established for and associated with a particular user and a particular application. The certificate preferably includes a pointer to its associated application, an identity of the user associated with this certificate, and a pointer to the user private key associated with the user of this certificate and application. When an application needs to transmit an encrypted message or to perform an authentication procedure, encryption/decryption engine 32 accesses the user private key pointed to by the application's associated certificate, and then encrypts the message or signs a signature utilizing the user private key. (column 3, line 55 to column 4, line 6)

As such, each user has a public/private key pair. However, nowhere does Challener state that this public/private key is generated from a user-supplied unencrypted password. Further, Challener does not disclose that this public/private key pair is provided from a user computing device.

With the key, again a public/private key pair, Challener starts a procedure illustrated in FIG. 2a to "associate a password with a user public/private key" (please see brief description of FIG. 2A, column 2, lines 64-65). The next cited portion of Challener reads:

> With reference now to FIG. 2a, there is illustrated a high-level logic flow diagram of a method for associating a password with a secured user public/private key pair, in accordance with a preferred embodiment of the present invention. Starting at block 40, a user public/private key pair is first received by a signature chip (such as signature chip 31 from FIG. 1), as shown in block 41. Typically, this user public/private key pair has already been certified with the proper authority. A random password, preferably 64 bits in length, to be associated with the user public/private key pair is then generated for the user, as depicted in block 42. This random password, which is preferably generated by a random generator, is typically very difficult for a human user to remember. Utilizing a chip public key, the random password is then encrypted along with the user public/private key pair, as shown in block 43. The chip public key may come from an unprotected or protected storage area of the signature chip. The encrypted package of the random password and user public/private key pair is then stored in a hard disk, such as SCSI disk drive 19 as shown in FIG. 1. At this point, any record of the user public/private key pair outside the signature chip can be discarded (by the human user) for security reasons, as depicted in block 44. (column 4, lines 7-29)

As such, a chip public key is used to encrypt a random password and the public/private key pair. Similar to the public/private key pair, the chip key is not described as being generated from a user-supplied unencrypted password. Next a password (hashed from a pass phrase) is encrypted with the random password. To perform this encryption, the chip public key is used. In this regard, the next cited portion of Challener reads:

> Next, a first password is generated by hashing a first pass phrase, as shown in block 45. A pass phrase is utilized because a pass phrase permits greater permutation, and thus added security, not to mention a pass phrase is easier for a human user to remember than the random password. Utilizing the chip public key, the first password is then encrypted along with the random password, as depicted in block 46. The encrypted package of the first password and random password can then also be stored in the hard disk. At this point, any record of the random password outside the signature chip can also be discarded (by the human user) for security reasons, as illustrated in block 47. (column 4, line 30-41)

As such, a password is encrypted with the public chip key, which similar to the user public/private key, is not described as being generated from a user-supplied unencrypted password (that is provided from a user computing device). With the password encrypted, Challener is now ready to use this data to challenge a would-be user. In particular, the encrypted password is decrypted and compared to a password associated with a would-be user. In this regard, Challener states:

> During operation, a first pass phrase sent by a user is hashed by a processor, such as processor 12 in FIG. 1, in a system memory, such as RAM 14 in FIG. 1, to obtain its corresponding first password. This first password along with the encrypted package of the first password and random password (from the hard disk) are then sent to the signature chip. The signature chip decrypts the encrypted package of the first password and random password. The signature chip then compares the first password from the decrypted package of the first password and random password with the sent first password. The signature can use the random password in the decrypted package if both first passwords match with each other. Because the random password is much less than 1,024 bits, the signature chip recognizes that the random password is not a signature key (i.e., the user private key of the user public/private key pair), and hence exports the random password to the system memory. The random password is subsequently sent to the signature chip along with a copy of the encrypted user public/private key pair stored in the hard drive to authorize the signature chip to perform a signatory function using the user private key.

As such, the password encrypted with the public chip key is decrypted for being compared to a password attainted from a pass phrase of a would-be user. Thus, Challener describes the use of a public/private key pair and a public chip key for performing the password comparison procedure. However, neither the public/public key pair nor the public chip key is generated "from a user-supplied unencrypted password," as required by independent claim 1.

Furthermore, neither the public/public key pair nor the public chip key is provided by a user computing device," also required by independent claim 1.

For at least these reasons, amended independent claim 1 is believed to be patentable over the Challener reference. Similarly, amended independent claims 7 and 11 are also believed to be allowable for at least the same reasons noted above. The dependent claims 2-6, 8-10 and 12 respectively partake of the novelty of their parent independent claims and, as such, have not been addressed specifically herein.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the foregoing remarks, the entire application is now believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience. Applicants' attorney can be reached at the address shown below. Telephone calls regarding this application should be directed to 617-368-2191.

No fees are believed due. Please apply any other charges or credits to deposit account 06 1050, referencing Attorney Docket No. 13984-0005US1.

Respectfully submitted,

Date: 7 March 2011

Jeffrey J. Barclay
Reg. No. 48,950

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945